IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Yi-Fen Chen et al.

Application No.:	10/829,466	Examiner:	Truong, Thanhnga B.
Filing Date:	April 21, 2004	Art Unit:	2135

Assignee: Trend Micro, Inc.

Title: METHOD AND APPARATUS FOR CONTROLLING TRAFFIC IN A COMPUTER NETWORK

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF FILED UNDER 37 C.F.R. § 41.37

Sir:

This appeal brief follows the Notice of Appeal submitted by Applicants on September 23, 2008.

The fee for filing an appeal brief is submitted herewith. If for any reason the fee is insufficient or additional fees are required, the Commissioner is hereby authorized to charge the insufficiency to Deposit Account No. 50-2427.

I. REAL PARTY IN INTEREST

The real party in interest is Trend Micro, Inc., which is the assignee of the present application.

II. RELATED APPEALS AND INTERFERENCES

On information and belief, there are no appeals, interferences, or judicial proceedings known to the appellant, the appellant's legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board of Patent Appeals and Interferences decision in the pending appeal.

III. STATUS OF ALL CLAIMS

A. Total Claims: 1-20

B. Current Status of Claims:

1. Claims canceled: none
2. Claims withdrawn: none
3. Claims pending: 1-20
4. Claims allowed: none
5. Claims rejected: 1-20
6. Claims objected to: none

C. Claims on Appeal: 1-20

IV. STATUS OF AMENDMENTS

No amendment has been filed after the Final Office Action mailed June 26, 2008 (final office action).

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 recites a method of controlling traffic in a computer network. In the embodiment of claim 1, data to be sent by a first computer is intended for a second computer but modified such that the data is redirected from the first computer to a third computer (Specification, page 12, line 22 to page 13, 2; page 14, line 19 to page 15, line 4; FIG. 7, DPDD 702; FIG. 8, packet 800). The data is generated and originates from the

first computer and being sent by the first computer to connect to the computer network (Specification, page 13, lines 3-8). The data is sent from the first computer to the third computer, and forwarded from the third computer to the second computer (Specification, page 13, lines 2 and 3).

Independent claim 10 recites a system for controlling traffic in a computer network. In the embodiment of claim 10, a first computer includes a kernel driver that is configured to modify a packet generated at the first computer such that the packet, which is intended for a second computer, is forwarded from the first computer to a third computer (Specification, page 11, line 20 to page 12, line 8; page 12, line 22 to page 13, line 8; FIG. 7, DPDD 702; FIG. 8, packet 800).

Independent claim 17 recites a method of controlling traffic in a computer network. In the embodiment of claim 17, a DHCP packet is modified at a first computer prior to initialization of a network-enabled application in the first computer (Specification, page 13, lines 3 to 10). The packet is intended for a DHCP server but modified to be redirected to a second computer, where the packet is processed prior to being forwarded to the DHCP server (Specification, page 15, lines 5-17; page 15, line 20 to page 16, line 6).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following are to be reviewed on appeal:

1) The rejection of claims 1-6, 8, 9, 17, 19, and 20 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,028,335 to Borella et al. and further in view of U.S. Patent No. 6,650,641 to Albert et al.

2) The rejection of claims 10 and 12-15 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,028,335 to Borella et al.

3) The rejection of claims 7, 11, 16, and 18 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,028,335 to Borella et al. in view of U.S. Patent No. 6,650,641 to Albert et al. and further in view of U.S. Patent No. 6,717,943 to Schwering.

VII. ARGUMENT

Applicants traverse the rejection of claims 1-20 for the following reasons.

A. CLAIMS 1, 2, 4, 7, 8 and 9

Claims 1-6, 8, 9, 17, 19, and 20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,028,335 to Borella et al. ("Borella") and further in view of U.S. Patent No. 6,650,641 to Albert et al. ("Albert"). The rejection is respectfully traversed.

Claim 1 pertains to sending of a data unit from a first computer to a second computer ("the data unit intended for a second computer"). Prior to sending the data unit from the first computer ("modifying a data unit to be sent by a first computer"; i.e., future tense), the data unit is modified such that it is redirected from the first computer to a third computer. The first computer then sends the data unit to the third computer ("sending the data unit from the first computer to the third computer"), which then forwards the data unit to the second computer ("forwarding the data unit from the third computer to the second computer").

In marked contrast, Borella does not pertain to modification of a data unit for redirection prior to being sent by the sender. In fact, Borella teaches away from packet modification, especially in a NAT router.

> A NAT router typically needs to modify an IP packet (e.g., network ports, etc.). However, once an IP packet is protected by IPSEC, it must not be modified anywhere along a path from an IPSEC source to an IPSEC destination.
>
> (Borella, col. 3, lines 38-42; emphasis added).

This is not surprising given that Borella advocates distributed network address translation by creating security associations between network devices using tables, not packet modification (Borella, Abstract; col. 4, lines 23-55). Albert cannot fix the deficiencies of Borella as it also pertains to conventional network address translation.

Claim 1 is patentable over the combination of Borella and Albert at least for reciting: "modifying a data unit to be sent by a first computer, the data unit being

intended for a second computer, the data unit being modified such that the data unit is redirected from the first computer to a third computer, the data unit being generated in and originating from the first computer and being sent by the first computer to connect to the computer network." It is respectfully submitted that Borella, Albert, or their combination does not teach or suggest such data modification at the sender of the data to redirect the data. Borella and Albert cannot meet the limitations of claim 1 as both do not involve packet modification in the computer where the packet is generated and originates.

The final office action cites to Borella col. 3, lines 37-42, and col. 4, lines 23-35 and 45-55. These cited sections of Borella do not teach or suggest modifying a data unit for redirection in the same computer ("first computer in claim 1") where the data unit is generated and originates as recited in claim 1.

- Borella col. 3, lines 37-42 discuss NAT routers that violate IPSEC protocol by modifying packets it receives from an IPSEC source. These NAT routers do not modify for redirection a packet generated by and originating from the NAT router itself.

- Borella col. 3, lines 37-42 specifically teach away from modifying packets in a NAT router. Borella is explicit that:

  > "However, once an IP packet is protected by IPSEC, it must not be modified anywhere along a path from an IPSEC source to an IPSEC destination" (Borella, col. 3, lines 38-42; emphasis added).

- Borella col. 4, lines 23-35 and 45-55 discuss packet distribution by using tables, not packet modification (unlike prior art NAT routers discussed in col. 3, lines 37-42). In any event, this section or any other section of Borella does not disclose a NAT router that modifies for redirection packets that the NAT router generates and originates.

Therefore, claim 1 is patentable over the combination of Borella and Albert.

Claim 1 is also patentable over the combination of Borella and Albert at least for reciting: "sending the data unit from the first computer to the third computer; and forwarding the data unit from the third computer to the second computer." That is, after

the data unit has been modified at the first computer (where the data unit is generated and originates from), the data unit is sent from the first computer to the third computer, and then from the third computer to the second computer, which is the data unit's intended destination. It is respectfully submitted that the combination of Borella and Albert does not teach or suggest such redirection of data unit.

The final office action cites to Borella col. 3, lines 24 and 25, col. 21, lines 51-53, and col. 4, lines 41-45. These sections of Borella are addressed as follows.

- Borella col. 3, lines 24 and 25 discuss data transmission under the IPSEC protocol. This section merely states that under IPSEC, one computer sends the packets and another endpoint receives the packets. This section has nothing to do with packet redirection by modifying the packet at a first computer for redirection to a third computer, and forwarding the packet from the third computer to the second computer, which is the intended destination of the packet from the first computer.
- Borella col. 21, lines 51-53 again simply talks about data transmission between two endpoints under IPSEC. Note that packet modification is not allowed between these two endpoints under IPSEC (Borella, col. 3, lines 38-42).
- Borella col. 4, lines 41-45 discuss Borella's embodiment, which does not perform packet modification. More importantly, this section discusses transmission from a third network device to a first network device, with a second network device intercepting the packet and forwarding the packet to the first network device if the security value has been allocated to the first network device i.e., the second network device performs interception and screening, not packet modification and redirection as claim 1 recites.

The above differences between Borella and claim 1 reflect their substantially different applications. Borella pertains to network address translation (see Borella, col. 4, lines 23-35) while claim 1 pertains to packet modification at the sender. For example, Borella needs an intermediary NAT device and cannot be implemented at the sender. Albert does not address the deficiencies of Borella because Albert also performs network address translation to route traffic.

Since Borella does not disclose packet redirection, the final office action suggests that "Albert correctly teaches data packet's redirection in Figures 6 and 10F and further details in col. 16, lines 27-41; column 28, lines 34-50 of Albert." Even so, this does not change the fact that neither Borella nor Albert discloses packet modification at the computer where the packet originates and is generated.

Therefore, for at least the above reasons, it is respectfully submitted that claim 1 is patentable over the combination of Borella and Albert.

Claims 2, 4, 8, and 9 depend on claim 1 and are thus patentable over the combination of Borella and Albert at least for the same reasons that claim 1 is patentable.

Claims 7, 11, 16, and 18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borella in view of Albert and further in view of U.S. Patent No. 6,717,943 to Schwering ("Schwering"). The rejection is respectfully traversed.

Claim 7 depends on claim 1 and is thus patentable over the combination of Borella, Albert, and Schwering at least for depending on patentable claim 1.

B. CLAIM 3

Claim 3 is patentable over the combination of Borella and Albert at least for reciting: "wherein the data unit is modified in the first computer prior to initialization of a network-enabled application in the first computer." It is respectfully submitted that neither Borella nor Albert can meet the limitations of claim 3 as both pertain to NAT routers, which have to be fully initialized to perform address translation.

The final office action cites to Borella col. 3, lines 37-42 and col. 4, lines 23-35 in the rejection of claim 3. These sections of Borella have been discussed above, and do not disclose anything relating to packet modification prior to initialization of a network-enabled application.

Therefore, it is respectfully submitted that claim 3 is patentable over the combination of Borella and Albert.

C. CLAIM 5

Claim 5 is patentable over the combination of Borella and Albert at least for reciting: "wherein a destination address field of the data unit is modified to contain an address of the third computer in a destination address field and an address of the second computer in another portion of the packet." It is respectfully submitted that Borella and Albert do not teach or suggest modifying a data unit to contain an address of the third computer (i.e., where the data unit is redirected) and an address of the second computer (i.e., where the data unit is intended to be sent) in another portion of the packet.

The final office action cites to Borella col. 19, lines 3-15. That section of Borella does not modify the received packet to change its address indicators. Instead, in that section of Borella, the packet is wrapped with an outer IP header for tunneling. That is, the received packet maintains its original addresses as is compliant with IPSEC (which prohibits packet modification). The packet is wrapped for routing, but not modified.

Therefore, it is respectfully submitted that claim 5 is patentable over the combination of Borella and Albert.

D. CLAIM 6

Claim 6 is patentable over the combination of Borella and Albert at least for reciting: "wherein the second computer comprises a DHCP (Dynamic Host Configuration Protocol) server." It is respectfully submitted that Borella and Albert does not teach or suggest redirection from a DHCP server (i.e., the second computer, which is the intended destination of the data unit).

The final office action cites to col. 10, lines 5-14 of Borella. That section of Borella discloses DHCP in general. That section of Borella does not teach or suggest redirection from a DHCP server as recited in claim 6.

Therefore, it is respectfully submitted that claim 6 is patentable over the combination of Borella and Albert.

E. CLAIMS 10, 11, 12, 13, 16

Claims 10 and 12-15 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Borella. The rejection is respectfully traversed.

Claim 10 is patentable over Borella at least for reciting: "a first computer including a kernel driver, the kernel driver being configured to modify a packet generated at the first computer, the packet being intended for a second computer and being modified to be forwarded from the first computer to a third computer" (emphasis added). The plain language of claim 10 requires a first computer that modifies a packet generated at the first computer. The packet, which is intended for a second computer, is modified at the first computer so that it is forwarded from the first computer to a third computer. As explained above, Borella does not teach or suggest packet modification for redirection at the computer where the packet is generated.

The final office action cites to Borella col. 3, lines 37-42, col. 4, lines 23-35, col. 3, lines 24 and 25, col. 21, lines 51-53, and col. 4, lines 41-45. These sections of Borella have been addressed above. As explained, these sections of Borella do not teach or suggest packet modification for redirection at the computer from which the packet originates. Borella pertains to routing of packets originated by other computers.

In the Response to Arguments, the final office action suggests that Borella discloses a kernel driver to modify packets, citing to Borella col. 8, lines 30-40, col. 14, line 56 to col. 15, line 17. There are at least two problems with this conclusion. Firstly, these sections pertain to the use of a NIC driver to wrap an IP header on a packet. Note that this function is performed by the NAT router, not on the computer where the packet is generated as required by claim 10. Secondly, the NIC driver in Borella does not modify the packet. It does not because packet modification is not allowed in IPSEC (Borella, col. 3, lines 37-42), which Borella uses. Instead, the NIC driver wraps the packet within an IP header (Borella, col. 15, lines 11-17) – the packet itself is not modified.

For at least the above reasons, it is respectfully submitted that claim 10 is patentable over Borella.

Claims 11, 12, 13, and 16 depend on claim 10.

Claim 12 and 13 are patentable over Borella at least for the same reasons that claim 10 is patentable.

Claims 11 and 16 are patentable over the combination of Borella, Albert, and Schwering at least for depending on patentable claim 10.

F. CLAIM 14

Claim 14 is patentable over Borella at least for reciting: "wherein the packet is modified at the first computer prior to initialization of a network-enabled application in the first computer." As explained with reference to claim 3, it is respectfully submitted that neither Borella nor Albert can meet the limitations of claim 14 as both pertain to NAT routers, which have to be fully initialized to perform address translation.

G. CLAIM 15

Claim 15 is patentable over Borella at least for reciting: "wherein the packet is modified to contain an address of the third computer in a destination address field of the packet and an address of the second computer in another portion of the packet." As explained with reference to claim 5, Borella and Albert do not teach or suggest modifying a data unit to contain an address of the third computer (i.e., where the data unit is redirected) and an address of the second computer (i.e., where the data unit is intended to be sent) in another portion of the packet.

H. CLAIMS 17 and 18

Claim 17 is patentable over the combination of Borella and Albert at least for reciting: "modifying a DHCP (dynamic host configuration protocol) packet at a first computer prior to initialization of a network-enabled application in the first computer, the DHCP packet being intended for a DHCP server, the DHCP packet being modified to be redirected to a second computer." Claim 17 further recites processing the packet at the second computer and forwarding the packet from the second computer to the DHCP server.

The final office action rejects claim 17 using the same rationale applied against claim 1. The patentability of claim 1 has been explained above.

Unlike claim 1, claim 17 recites modification of DHCP packets in a computer prior to initialization of a network-enabled application in the first computer. It is

respectfully submitted that Borella does not pertain to DHCP packet modification at all. The final office action cites to col. 10, lines 5-14 of Borella in the rejection of claim 6. However, that section of Borella merely discloses DHCP in general. That section of Borella does not teach or suggest modification of a DHCP packet in a first computer prior to initialization of a network-enabled application in the first computer, such that the DHCP packet is processed at another computer ("second computer" in claim 17) prior to being received at the DHCP server.

For at least the above reasons, it is respectfully submitted that claim 17 is patentable over the combination of Borella and Albert.

Claim 18 depends on claim 17. Claim 18 is patentable over the combination of Borella, Albert, and Schwering at least for depending on patentable claim 17.

I. CLAIM 19

Claim 19 is patentable over the combination of Borella and Albert at least for reciting: "wherein modifying the packet at the first computer comprises including an address of the second computer in a destination address field of the packet and including an address of the DHCP server in another portion of the packet."

As explained with reference to claim 5, Borella and Albert do not teach or suggest modifying a data unit to contain an address of the second computer (i.e., where the data unit is redirected) and an address of the DHCP server computer (i.e., where the data unit is intended to be sent) in another portion of the packet.

J. CLAIM 20

Claim 20 is patentable over the combination of Borella and Albert at least for reciting: "forwarding a response packet from the DHCP server to the first computer after the packet is forwarded from the second computer to the DHCP server."

The final office action suggests that claim 20 is similar to another claim in the present application. Applicants respectfully disagree with this conclusion. Claim 20 pertains to response packets from DHCP servers. In particular, claim 20 recites that the DHCP server forwards a response packet to the first computer, where the DHCP packet is modified for redirection to the second computer according to claim 17.

In any event, it is respectfully submitted that the combination of Borella and Albert does not teach or suggest forwarding a response packet from a DHCP server to the computer where a packet for the DHCP server was modified for redirection.

VIII. CLAIMS INVOLVED IN THE APPEAL

Claims 1-20 are involved in the appeal. These claims involved in the appeal are included in the Appendix submitted herewith.

IX. CONCLUSION

For at least the above reasons, allowance of claims 1-20 is respectfully requested.

Respectfully submitted,
Yi-Fen Chen et al.

Dated: November 3, 2008

/Patrick D. Benedicto, Reg. No. 40,909/
Patrick D. Benedicto, Reg. No. 40,909
Okamoto & Benedicto LLP
P.O. Box 641330
San Jose, CA 95164
Tel.: (408)436-2110
Fax.: (408)436-2114

CLAIMS APPENDIX

CLAIMS INVOLVED IN THE APPEAL

1. A method of controlling traffic in a computer network, the method comprising:
modifying a data unit to be sent by a first computer, the data unit being intended for a second computer, the data unit being modified such that the data unit is redirected from the first computer to a third computer, the data unit being generated in and originating from the first computer and being sent by the first computer to connect to the computer network;
sending the data unit from the first computer to the third computer; and
forwarding the data unit from the third computer to the second computer.

2. The method of claim 1 wherein the data unit is selected to be modified based on an intended destination of the data unit.

3. The method of claim 1 wherein the data unit is modified in the first computer prior to initialization of a network-enabled application in the first computer.

4. The method of claim 1 wherein the data unit comprises an Ethernet packet.

5. The method of claim 1 wherein a destination address field of the data unit is modified to contain an address of the third computer in a destination address field and an address of the second computer in another portion of the packet.

6. The method of claim 1 wherein the second computer comprises a DHCP (Dynamic Host Configuration Protocol) server.

7. The method of claim 1 further comprising:
scanning the data unit for viruses at the third computer.

8. The method of claim 1 wherein the data unit is quarantined at the third computer.

9. The method of claim 1 wherein the third computer is selected to receive the data unit based on an intended destination of the data unit.

10. A system for controlling traffic in a computer network, the system comprising:
a first computer including a kernel driver, the kernel driver being configured to modify a packet generated at the first computer, the packet being intended for a second computer and being modified to be forwarded from the first computer to a third computer.

11. The system of claim 10 wherein the third computer is configured to scan the packet for viruses prior to forwarding the packet from the third computer to the second computer.

12. The system of claim 10 wherein the packet comprises an Ethernet packet.

13. The system of claim 10 wherein the packet is selected to be modified based on the packet's intended destination computer.

14. The system of claim 10 wherein the packet is modified at the first computer prior to initialization of a network-enabled application in the first computer.

15. The system of claim 10 wherein the packet is modified to contain an address of the third computer in a destination address field of the packet and an address of the second computer in another portion of the packet.

16. The system of claim 10 wherein the third computer includes a scanning engine for scanning the packet for viruses.

17. A method of controlling traffic in a computer network, the method comprising:
modifying a DHCP (dynamic host configuration protocol) packet at a first computer prior to initialization of a network-enabled application in the first computer, the DHCP packet being intended for a DHCP server, the DHCP packet being modified to be redirected to a second computer;
processing the packet at the second computer; and
forwarding the packet from the second computer to the DHCP server.

18. The method of claim 17 wherein processing the packet at the second computer includes scanning the packet for viruses.

19. The method of claim 17 wherein modifying the packet at the first computer comprises including an address of the second computer in a destination address field of the packet and including an address of the DHCP server in another portion of the packet.

20. The method of claim 17 further comprising:
forwarding a response packet from the DHCP server to the first computer after the packet is forwarded from the second computer to the DHCP server.

EVIDENCE APPENDIX

There are no documents or items submitted under this section.

RELATED PROCEEDINGS APPENDIX

There are no documents or items submitted under this section.